

中国认证认可协会文件

中认协注 [2009] 231 号

关于发布《信息安全管理体系统认证咨询师注册准则》的通知

各相关认证咨询机构及注册申请人：

为促进信息安全管理体系统（ISMS）认证咨询工作，满足认证咨询机构对认证咨询师的需求，我会建立了 ISMS 认证咨询师注册制度，制订了《信息安全管理体系统认证咨询师注册准则》（见附件），现予发布实施。

特此通知。

附件：

《信息安全管理体系统认证咨询师注册准则》

二 九年九月十一日

中国认证认可协会



信息安全管理体系
认证咨询师注册准则

第 1 版

文件编号：CCAA-133

发布日期：2009 年 9 月 9 日

©版权 2009-中国认证认可协会

信息安全管理体系认证咨询师注册准则

类别

本准则为 CCAA 规范类文件。

本准则规定了 CCAA 运作其认证咨询师注册项目时遵循的原则。

本准则经 CCAA 批准发布。

批准

第 1 版

实施日期：2009 年 9 月 9 日

编制：CCAA

日期：2009 年 8 月 18 日

批准：CCAA

日期：2009 年 9 月 9 日

信息

所有 CCAA 文件都用中文发布。标有最近发布日期的中文版 CCAA 文件是有效的版本。CCAA 将在 CCAA 网站上公布所有 CCAA 相关准则的最新版本。

关于 CCAA 或 CCAA 认证咨询师注册的更多信息，请与 CCAA 联系联络地址如下：

地址：北京市朝阳区朝外大街甲 10 号中认大厦 13 层

邮编：100020

电子邮箱：pcc@ccaa.org.cn

版权

©版权 2009-中国认证认可协会

前 言

本准则由 CCAA 依据国家质量监督检验检疫总局《认证及认证培训、咨询人员管理办法》（质检总局令第 61 号）和《认证咨询机构管理办法》（质检总局令第 82 号），参考了目前国家认证认可监督管理委员会批准开展的信息安全管理体系（ISMS）认证标准、实施规则，结合 CCAA 已经开展的质量管理体系认证咨询师、环境管理体系认证咨询师和职业健康安全管理体系认证咨询师注册实践而制定。目的是为 ISMS 认证咨询师注册提供一个基础性的规范。

本准则规定了 CCAA ISMS 认证咨询师的注册要求，以及注册过程的要求。

CCAA ISMS 认证咨询师的注册仅表明注册人员具备从事 ISMS 认证咨询的相应的知识和能力，不对注册人员的专业技术范围和能力加以识别和确认。尽管 CCAA 已尽力保证评价考核过程和注册制度的科学性和有效性，但如果某一注册人员提供的咨询或其它服务未能满足客户的所有要求，CCAA 对此不承担责任。

所有 CCAA 文件都用中文发布。标有最近发布日期中文版 CCAA 的文件是有效的版本。CCAA 将在 CCAA 网站上公布所有 CCAA 相关准则的最新版本。

第一章 概论

1.1 引言

1.1.1 本准则由中国认证认可协会（CCAA）制定，目的是促进我国 ISMS 认证咨询工作健康、有序地发展，规范我国 ISMS 认证咨询师的注册活动。

1.1.2 本准则的作用是建立和完善 CCAA ISMS 认证咨询师的注册制度，规定 ISMS 认证咨询师的注册要求和方法。

1.2 引用文件

《认证及认证培训、咨询人员管理办法》（质检总局令第 61 号）；

《认证咨询机构管理办法》（质检总局令第 82 号）；

GB/T 19011-2003《质量和（或）环境管理体系审核指南》；

与 ISMS 认证有关实施规则 and 标准。

1.3 定义

本准则使用下列定义：

1.3.1 ISMS 的实现

ISMS 的建立、文件化、实施、保持和持续改进的过程

注：ISMS 的实现可包含以下内容：

- a) 根据业务特点、组织结构、位置、资产和技术，确定 ISMS 的范围和边界，ISMS 方针；
- b) 确定组织的风险评估方法，识别风险，分析评价风险，识别和评价风险处理的可选措施，为处理风险选择控制目标和控制措施；
- c) 为管理信息安全风险识别适当的管理措施、资源、职责和优先顺序，实施风险处理计划以达到已识别的控制目标，实施控制措施，以满足控制目标；
- d) 管理 ISMS 的运行；
- e) 执行监视和评审程序和其它控制措施；
- f) 在考虑安全审核结果、事故、有效性测量结果、所有相关方的建议和反馈的基础上，进行 ISMS 有效性的定期评审，测量控制措施的有效性以验证安全要求是否被满足；

- g) 按照计划的时间间隔进行风险评估的评审，以及对残余风险和已确定的可接受的风险级别进行评审；
- h) 按计划的时间间隔，对 ISMS 进行内部审核，定期对 ISMS 进行管理评审，以确保 ISMS 范围保持充分，ISMS 过程的改进得到识别，考虑监视和评审活动的结果，以更新安全计划。
- i) 实施已识别的 ISMS 改进，向所有相关方沟通行动和改进措施，确保改进达到了预期目标。

1.3.2 ISMS 认证咨询师

在组织的 ISMS 的实现方面给予帮助、提供建议或信息的人。

注：咨询师也可以在部分 ISMS 的实现方面提供帮助。

1.3.3 ISMS 认证咨询

为使 ISMS 符合相关认证标准和技术规范而提供的技术指导和服务。

1.3.4 ISMS 认证咨询经历

指导和帮助一个认证咨询客户完成一次 ISMS 实现的过程。

1.3.5 担保人

具有良好的个人品质，了解申请人专业背景并能够证明申请人个人素质和经历的具有 CCAA 认证人员注册资格（不含实习注册资格）的人员。

1.4 ISMS 认证咨询师注册级别

1.4.1 CCAA ISMS 认证咨询师注册分为实习认证咨询师、认证咨询师和高级认证咨询师三个级别。

- **ISMS 实习认证咨询师**

实习认证咨询师是指经 CCAA 评价确认，符合本准则相应注册资格要求，具备 ISMS 认证咨询相应知识和技能的人员。

实习认证咨询师可以在认证咨询师或高级认证咨询师的领导下，作为咨询组成员参与 ISMS 认证咨询活动。

- **ISMS 认证咨询师**

认证咨询师是指经 CCAA 评价确认，符合本准则相应注册资格要求，具备 ISMS 认证咨询相应知识和技能，并在实施认证咨询活动方面有一定经验的人员。

认证咨询师可以独立完成或领导咨询组完成 ISMS 认证咨询活动。

认证咨询师有责任指导咨询组内的实习认证咨询师实施和改进咨询活动。

● ISMS 高级认证咨询师

高级认证咨询师是指经 CCAA 评价确认,符合本准则相应注册资格要求,具备 ISMS 认证咨询相应的充分知识和技能,并具有丰富咨询经验和能力的人员。

高级认证咨询师可以独立完成或领导咨询组完成 ISMS 认证咨询活动。

高级认证咨询师有责任指导咨询组内的实习认证咨询师和认证咨询师实施和改进咨询活动。

1.4.2 CCAA ISMS 认证咨询师注册遵循逐级晋升原则。

第二章 注册要求

2.1 注册申请人资格要求

2.1.1 教育经历

2.1.1.1 各级别注册申请人应具有国家承认的信息安全相应专业(计算机科学技术、电子、通信和自动化控制技术、数学、物理)、或信息安全相关的其他理工科、或管理类专业的大学本科以上学历(含本科)。

2.1.2 工作经历

2.1.2.1 信息安全相应专业申请人应具有至少 4 年工作经历,信息安全相关专业申请人应具有至少 6 年工作经历,该工作经历应在负有判定责任、解决问题和与其他管理者或专业人员、同行及顾客进行沟通的技术、专业或管理岗位上获得。

2.1.2.2 满足注册要求的工作经历应在取得相应学历后获得。

2.1.2.3 申请人应提交工作经历的书面证明。证明中应提供申请人从事的工作职责、岗位、级别。

注1:工作经历是指管理相关的技术、专业工作岗位经历。原则上,某一组织中相关的管理职能部门的人员以及与实施部门的负责人经历被视为认证咨询师注册时可接受的工作经历。

注2:实施部门具体岗位的操作人员(如:销售人员、医疗护理人员、财务出纳、设备操作人员、服务行业从事具体服务的人员等)其经历不能作为认证咨询师注册时可接受的工作经历。

2.1.3 信息安全管理工作经历

2.1.3.1 申请人在全部工作经历中应具有至少 2 年与信息安全管理相关的经历,且为

最近从事的工作经历。

2.1.3.2 适宜的信息安全管理经历包括 ISMS 的实施、运作、咨询、审核和科研教学等经历。

2.1.4 ISMS 认证咨询经历

2.1.4.1 实习认证咨询师申请人无 ISMS 认证咨询经历要求。

2.1.4.2 认证咨询师申请人的 ISMS 认证咨询经历要求：

作为认证咨询组成员，成功地完成至少 2 次 ISMS 认证咨询经历。

2.1.4.3 高级认证咨询师申请人的 ISMS 认证咨询经历要求：

作为认证咨询组组长，成功地完成至少 2 次 ISMS 认证咨询经历。

2.1.4.4 注册接受的 ISMS 认证咨询经历

1) 一个 ISMS 认证咨询经历应包括下列活动中的至少 4 项：

- 调研诊断
- 体系策划
- 人员培训
- 文件编制
- 体系运行与维护
- 内部审核或符合性审核
- 管理评审

2) ISMS 认证咨询经历应在提交注册申请前 3 年内获得；

3) ISMS 认证咨询经历涉及的认证咨询客户应在完成咨询后成功获得相应的认证证书。

2.1.4.5 认证咨询经历记录

2.1.4.5.1 认证咨询师和高级认证咨询师注册和再注册应随申请附上认证咨询经历记录。记录应至少包含下列信息：

- 1) 认证咨询开始的日期和持续的时间；
- 2) 认证咨询依据的 ISMS 标准；
- 3) 认证咨询经历包括的活动[见 2.1.4.4 1)]；
- 4) 认证咨询组成员人数；
- 5) 申请人在认证咨询组中的身份、作用和承担的工作；
- 6) 咨询客户的名称和联系信息（地址、邮政编码，管理者代表和电话）；

2.1.4.5.2 认证咨询经历记录应使用 CCAA 指定的统一表格。

2.2 个人素质要求

2.2.1 各级别注册申请人应具备下列个人素质：

- 1) 有道德：公平、诚实、忠诚、正直和谨慎；
- 2) 善于观察：能经常和主动了解组织的文化和价值观、周围环境和活动；
- 3) 有感知力：能够了解和理解对于变更和改进的需求；
- 4) 适应力强：能适应不同的环境，并能提供可供选择的和创造性的解决办法；
- 5) 坚忍不拔：为实现目标而坚持不懈；
- 6) 明断：能够根据逻辑推理和分析及时得出结论；
- 7) 自立：能够在同其他人的有效交往中独立工作并发挥作用；
- 8) 善于沟通：能与组织各层次进行有效地接触，听取他们的意见，信赖组织的文化并保持敏感性；
- 9) 有实践经验：有良好且灵活的实际管理经验；
- 10) 有责任感：能对自身的行为负责；
- 11) 乐于助人：能够自始至终在 ISMS 的实现中，为组织的管理者和员工提供帮助。

2.3 知识和技能要求

2.3.1 各级别认证咨询师申请人应具备以下知识和技能

2.3.1.1 信息安全管理专业知识和技能

- 1) 正确理解和有效应用信息安全管理体制相关标准：
 - GB/T 22080-2008 / ISO/IEC27001:2005 《信息技术 安全技术 信息安全管理体系 要求》
 - GB/T 22081-2008 / ISO/IEC27002:2005《信息技术 安全技术 信息安全管理体系实用规则 》
 - ISO/IEC 27005 :2008 《信息技术 安全技术 信息安全风险管理》
- 2) 正确理解、掌握和适当应用信息安全管理体制相关的原则、方法和技术：
 - 信息安全管理原则；
 - 风险评价和风险控制原理和方法；

- 信息安全技术，特别是 GB/T 22081-2008 / ISO/IEC27002:2005 所涉及的相关技术；
- 信息安全法规知识；
- 审核的方法和技术、PDCA 方法等；
- 团队工作的技巧；
- 解决问题的技巧；
- 监视顾客和员工满意度的方法；

2.3.1.2 与组织运作有关的知识和技能

- 1) 了解与组织运作活动相关的法律法规要求；
- 2) 了解组织所开展的各类工作活动及与工作活动相关的信息安全问题；
- 3) 理解组织所在部门的术语；
- 4) 理解组织结构、职能和相互关系的性质；
- 5) 了解 ISMS 与组织的整体管理进行整合和相互作用，具备相关的管理实践知识；
- 6) 理解经营目标和所需的能力资源需求之间的战略关系。

2.3.1.3 认证咨询程序、过程和方法的知识和技能

掌握认证咨询过程和方法，包括：调研诊断、体系策划、人员培训、文件编写、文件发布、体系运行、内部审核、管理评审和符合性审核等。

2.3.1.4 认证认可的知识的过程

- 1) 了解国家认证认可的法律法规；
- 2) 了解国家认证认可制度，掌握管理体系认证的过程和程序及相关标准；
- 3) 了解 ISO/IEC 27006 《信息安全管理体系认证机构的认可要求》；
- 4) 了解 GB/T 27021 《合格评定—对管理体系认证机构的要求》等。

2.3.1.5 高级认证咨询师还应具备以下任一种要求

- 1) 中级以上技术职称；或
- 2) 硕士以上学历（含硕士）；或
- 3) 在国家批准的正式出版物发表过与信息安全工作有关的文章；

2.3.2 注册考试

2.3.2.1 实习认证咨询师申请人应参加咨询师注册考试，并成绩合格，以证实其具备了 ISMS 认证咨询相应的知识；

2.3.2.2 考试范围为本准则 2.3.1 知识和技能要求的内容，以及 2.2 个人素质涉及的适当内容。

2.4 申请资料要求

2.4.1 所有申请人应认真阅读 CCAA 注册准则，如实填写申请材料，对所填内容的真实性负责。

2.4.2 所有申请人应签署声明，表示愿意遵守 CCAA 认证咨询师行为规范和注册准则各项要求。

2.4.3 所有申请人应使用 CCAA 统一表格，在 CCAA 网上下载申请表或在注册系统填写后直接打印申请表格，应完成其中的全部内容，由本人亲笔签字，担保人签字，附上所有要求的证明材料。

2.4.3.1 实习咨询师注册申请资料包括：

- 1) 认证咨询师注册申请表（原件，贴一张相片）；
- 2) 教育经历证明；
- 3) ISMS 咨询师考试合格证明（复印件）；

2.4.3.2 咨询师注册申请资料包括：

- 1) 认证咨询师注册申请表（原件，贴一张相片）；
- 2) 实习认证咨询师证书或注册公告（复印件）；
- 3) ISMS 认证咨询经历证明（见 2.1.4.5），包括：
 - CCAA 认证咨询经历记录表（原件）；
 - 客户通过认证的证书（复印件）。

2.4.3.3 高级咨询师注册申请资料包括：

- 1) 认证咨询师注册申请表（原件，贴一张相片）；
- 2) 职称、教育经历或发表文章的证明；
- 3) 认证咨询师证书或注册公告（复印件）；
- 4) CCAA 认证咨询经历证明（见 2.1.4.5），包括：
 - CCAA 认证咨询经历记录表（原件）；
 - 客户通过认证的证书（复印件）；

5) 完成历次年度确认的证明（适用时）。

2.5 担保

2.5.1 每名注册申请人应由一名担保人担保（参见 1.3 担保人定义）。

2.5.2 担保人应对申请人个人素质的适宜性和信息安全管理工作经历的真实性作出担保。

2.6 认证咨询师行为规范

各级别认证咨询师有义务遵守以下行为规范。不能遵守以下要求，可导致暂停或撤销注册资格。

- 1) 遵纪守法、敬业诚信；
- 2) 努力提高认证咨询专业能力；
- 3) 对咨询客户提供的或从咨询客户获得的信息保密；
- 4) 不得干涉咨询客户自主选择认证机构的权力；
- 5) 不得承担超过业务范围和能力的认证咨询工作；
- 6) 不得为咨询客户编造体系文件运行记录或者帮助、授意咨询客户隐瞒自身实际情况；
- 7) 不得介入认证机构对咨询客户的审核活动；
- 8) 在任何情况下，不损害 CCAA 及其注册过程的声誉，与针对违反本准则的行为所做的调查进行全面合作。

2.7 监督与年度确认

2.7.1 CCAA 采用年度确认的方式，对咨询师和高级咨询师持续保持其能力和个人素质以及遵守行为规范的情况进行监督。

2.7.2 认证咨询师和高级认证咨询师每年应进行一次年度确认，表明其：

- 至少完成 1 次 ISMS 认证咨询经历；
- 持续遵守行为规范的要求；
- 与咨询工作有关的表彰或已妥善解决任何针对其咨询表现的投诉；
- 当 CCAA 有指定的专业发展活动时，已按要求完成。

2.7.3 认证咨询师和高级认证咨询师应保留与 2.7.2 条款相一致的用于年度确认的

ISMS 认证咨询经历记录(原件)和完成年度确认的证明文件(如 CCAA 年度确认通知), 在申请再注册时提交 CCAA。

2.7.4 实习认证咨询师无年度确认要求。CCAA 将通过处理投诉、向聘用机构和接受咨询的组织收集信息等方式进行监督。

2.7.5 必要时, CCAA 可对各级别咨询师采取专项调查、质询或要求提供更多证实信息等方式进行更频繁更深入的监督。

2.8 再注册

2.8.1 实习认证咨询师、认证咨询师和高级认证咨询师再注册要求

2.8.1.1 实习认证咨询师、认证咨询师和高级认证咨询师应每 3 年进行一次再注册。再注册申请应于注册期满前 3 个月内向 CCAA 提交。新证书有效期 3 年, 自原注册证书截止日期延续计算。

2.8.1.2 实习认证咨询师、认证咨询师和高级认证咨询师应在证书有效期内持续符合本准则规定的相应要求。

2.8.1.3 认证咨询师和高级认证咨询师应在证书有效期内完成历次的年度确认以及专业发展(适用时); 实习认证咨询师无咨询经历和年度确认要求。

2.8.2 再注册申请资料包括:

- 1) 认证咨询师注册申请表(原件, 贴一张相片);
- 2) 原认证咨询师注册证书或注册公告(复印件);
- 3) ISMS 认证咨询经历证明(见 2.1.4.5), 包括:
 - ISMS 认证咨询经历记录表(原件);
 - 客户通过认证的证书(复印件)。
- 4) 完成历次年度确认的证明;
- 5) 专业发展证明(适用时)。

2.9 注册收费

2.9.1 CCAA 依据《认证人员注册、培训认可收费规则》收取注册相关费用, 注册申请人和已注册人员应遵照规则缴纳相应费用。

2.10 注册资格、证书的使用

2.10.1 经注册的各级别认证咨询师应遵守 CCAA 《证书及标志的使用规则》，并在取得注册证书之前签署《认证人员注册证书、标志使用承诺》。

第三章 注册过程

3.1 申请申报

3.1.1 实习认证咨询师、认证咨询师和高级认证咨询师注册申请由本人向 CCAA 申报，担保人对申请资料的真实性进行担保。

3.2 评价与考核

3.2.1 评价与考核人员

CCAA 依据《人员认证评价考核人员管理程序》选择评价考核人员，实施评价和考核。

3.2.2 受理申请

3.2.2.1 确认申请资料齐全，填写正确；

3.2.2.2 识别申请人是否有特殊需求，并作出适当安排。

3.2.3 申请人资格评价

3.2.3.1 教育经历评价

评价教育经历与准则 2.1.1 要求的符合性，可采用下列方式：

- 1) 原件，由评价与考核人员审阅后返还申请人；或
- 2) 上述原件的真实复印件；或
- 3) 由具有资格的权威机构以信函的方式确认申请人的证书是得到认可的。

3.2.3.2 工作经历、信息安全管理工作经历评价

评价工作经历、信息安全管理工作经历与准则 2.1.2 和 2.1.3 要求的符合性。包括：

- 组织的业务性质；
- 被聘用的起止日期；
- 聘用期间的职责。

3.2.3.3 ISMS 认证咨询经历评价

评价 ISMS 认证咨询经历的内容与准则 2.1.4 要求的符合性。

3.2.4 知识和能力考核

CCAA 依据《考试管理程序》和 2.3.2 的规定，组织实施认证咨询师注册考试，对申请人具备相关知识和技能的情况进行考核，以评价与准则 2.3.1 要求和 2.2 要求的符合性。

3.2.5 经验和能力考核

评价咨询经历和 2.3.1.5 所要求提供的证明与准则 1.4.1 中对高级咨询师的要求的符合性。

3.2.6 评价考核结论

评价考核人员根据资格评价和考试结果形成评价考核结论和注册推荐意见；

评价考核结论包括：

- 符合本准则各项要求，推荐注册；
- 存在一般不符合，采取有效的纠正/纠正措施关闭不符合，达到本准则各项要求，推荐注册；
- 存在严重不符合，建议不予注册，包括：
 - ◆ 个人素质存在明显缺陷；
 - ◆ 严重违反行为规范；
 - ◆ 存在短期内无法关闭的不符合；
 - ◆ 针对一般不符合所采取的纠正/纠正措施无效；
 - ◆ 考试不合格。

3.3 注册决定与批准

3.3.1 CCAA 注册管理人员对评价、考核各阶段工作进行审定，包括对评价考核过程中收集的信息的审定，对注册过程符合性的审定，并根据评价与考核结论做出是否予以注册的决定。必要时，可要求重新实施评价考核活动。

3.3.2 CCAA 负责人批准注册决定，必要时，可要求重新实施注册评价考核及认证决定等活动。

3.4 证书和/或公告

3.4.1 对经批准注册的申请人，CCAA 将予公告和/或颁发注册证书。

3.4.2 CCAA 负责人签发或批准人员注册公告。

3.4.3 CCAA 将发布注册人员名单/名录，注册人员对注册信息的公布有特殊要求的，须在递交申请书时予以书面说明。

3.4.4 注册证书内容应包括（适用时）：

- 注册人员的姓名；
- 身份识别代码；
- 注册准则标识；
- 注册级别；
- 注册编号；
- 注册日期；
- 注册有效期；
- CCAA 的名称、标志。

3.5 资格处置

对于不符合本准则相应要求的注册人员，CCAA 将依据文件化的程序对其注册资格进行处置，详见 CCAA 《注册人员资格处置规则》。

3.6 投诉与申诉

CCAA 制定文件化程序处理有关评价、考核和注册的投诉和申诉，详见 CCAA 《申诉、投诉和争议处理程序规则》。申请人可从 CCAA 网站下载该规则，CCAA 也可应申请人的请求提供该规则。

3.7 记录

CCAA 和注册人员应保存必要的记录，用以表明对本准则要求的符合性。这些记录保存期应按 CCAA 规定的期限执行。